UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/609,261	06/26/2003	Ramarathnam Venkatesan	MS1-1042US	8089

22801 7590 05/19/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/609,261	VENKATESAN ET AL.	
	Examiner	Art Unit	
	PETER POLTORAK	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/18/08 has been entered.

Response to Arguments

2. Applicant arguments are directed towards the newly introduced limitation, which required a new search and consideration. The search resulted in the newly discovered art: Boneh (Dan Boneh, Ben Lynn and Hovav Shacham, "Short signature from the Weil pairing" published December 9-13, 2001, Advances in Cryptology — ASIACRYPT 2001). The new rejection that incorporates Boneh's disclosure, below, addresses the newly introduced limitation.

3. Claims 1-20 have been examined.

Double Patenting

4. Claims 1-20 remain rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6, 8-18, 20-29, 31-40 and 42-47 U.S. Patent Application No. 10/609260.

Claim Rejections - 35 USC § 103

5. Claims 1-3, 8-10 and 15-17 is newly rejected under 35 U.S.C. 103(a) as being unpatentable over Boldyreva ("Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-group signature scheme", 2002) in view of Zhand (Fangguo Zhang and Kwangjo Kim, "ID-Based Blind Signature and Ring Signature from Pairings", 2002) and further in view of Boneh (Dan Boneh, Ben Lynn and Hovav Shacham, "Short signature from the Weil pairing" published December 9-13, 2001, Advances in Cryptology — ASIACRYPT 2001)

   Boldyreva discusses blind signatures using Gap-Diffie-Hellman (GDH) group of elements (e.g. "Abstract").
6. As per claims 1, 8 and 15, Boldyreva discloses receiving first data to be blindly signed; establishing parameter data for use with signature generating logic that encrypts data, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman group of elements relating to said curve; determining private key data and corresponding public key data using said signature generating logic; and generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature (e.g. "The blind GDH signature scheme, pg. 12).
7. Boldyreva discussion of blind GDH signatures also reads on claims 2-7.
8. Although, Boldyreva does not explicitly disclose encrypting data based on a Jaocbion of at least one curve, the examiner points out that the choice of encrypting data based on a Jacobian of at least one curve, would have been obvious to one of

ordinary skill in the art given that they are well known (e.g. Zhand on pg. 7) and barring any unexpected results.

9. Boldyreva does not explicitly teach computer readable medium and memory used in the data signing.

Zhand discloses real life applications of blind signatures, in which the computers are utilized (Zhand, "Introduction", pg. 1-2), and computers use memory to compute code stored on a readable medium. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize computers (that comprise computer readable medium and memory). One of ordinary skill in the art would have been motivated to perform such a modification in order to provide anonymity of users in electronic applications, such as electronic voiding and payment system. Furthermore, the examiner points out that an ordinary artisan would readily recognize the value of computers (with memory and readable medium for storing computer code) given the benefit of the inherent nature of computers to compute data.

10. Zhands disclosure discloses that "said blind digital signature corresponds to a single element in the Jacobian of the at least one curve" (see Response to Amendment, above). Furthermore, not only Zhands suggests dissemination of signatures (Zhands, 1.1), but also dissemination of digital signatures is well known in the art, and an ordinary artisan would have been motivated to implement it especially in light of the benefits of digital signatures as evidenced by their commercial success.

11. **As per newly introduced limitation,** Boldyreva in view of Zhand does not disclose that the digital signature has a length corresponding to a single element in the Jacobian of the at least one curve.

Boneh discloses a digital signature that has a length corresponding to a single element in the Jacobian of the at least one curve (see Boneh, "3.5 An open problem: short signatures with high security", in particular pg. 525).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a digital signature that has a length corresponding to a single element in the Jacobian of the at least one curve as disclosed by Boneh giving the benefit of give more variety in signature length .

Alternatively, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include Boldyreva in view of Zhand's invention into Boneh's invention comprising a digital signature that has a length corresponding to a single element in the Jacobian of the at least one curve given the benefit of offering a signature scheme secure against existential forgery under chosen message attack in the random oracle model.

12. Claims 9-14 and 16-20 are substantially equivalent to claims 2-7; therefore claim 9-14 and 16-20 are similarly rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PETER POLTORAK whose telephone number is (571)

272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Peter Poltorak/
Examiner, Art Unit 2134

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132